



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,477	07/14/2004	James E. Aston	014682.000010	4476
44870 7590 11/16/2007 MOORE & VAN ALLEN, PLLC For IBM P.O. Box 13706 Research Triangle Park, NC 27709			EXAMINER DWIVEDI, MAHESH H	
			ART UNIT 2168	PAPER NUMBER
			MAIL DATE 11/16/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/710,477

Applicant(s)

ASTON ET AL.

Examiner

Mahesh H. Dwivedi

Art Unit

2168

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 04 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-5 and 7-44 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-5, and 7-44 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 September 2003 is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

Art Unit: 2168

## DETAILED ACTION

### *Remarks*

1. Receipt of Applicant's Amendment filed on 09/04/2007 is acknowledged. The amendment includes the amending of claims 1, 9, 20-21, 28, 30, and 38, and the cancellation of claim 6.

### *Claim Objections*

2. The objections raised in the office action mailed on 06/06/2007 have been overcome by applicant's amendments received on 09/04/2007.

### *Claim Rejections - 35 USC § 112*

3. The rejections raised in the office action mailed on 06/06/2007 have been overcome by applicant's amendments received on 09/04/2007.

### *Claim Rejections - 35 USC § 101*

4. The rejections raised in the office action mailed on 06/06/2007 have been overcome by applicant's amendments received on 09/04/2007.

### *Claim Rejections - 35 USC § 102*

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-2, 5, 7-9, 12-19, 21-30, 32-38, and 40-44 are rejected under 35 U.S.C. 102(b) as being anticipated by **Halperin et al.** (U.S. PGPUB 2002/0194490).

7. Regarding claim 1, **Halperin** teaches a method comprising:

A) flagging a program on a computer as being suspect for possibly containing a virus in response to at least one of: opening a local file on a local file system of the computer to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system and at least the medium security level being set (Abstract, Paragraphs 73-77, and 88-108);

B) storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program (Paragraphs 108).

The examiner notes that **Halperin** teaches "**flagging a program on a computer as being suspect for possibly containing a virus in response to at least one of: opening a local file on a local file system of the computer to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the**

Art Unit: 2168

**local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system and at least the medium security level being set**” as “A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network” (Abstract), “After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2” (Paragraph 97-107), and “server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected” (Paragraphs 73-77). The examiner further notes that **Halperin** teaches **“storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program”** as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be “quarantined” at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages” (Paragraph 108).

Regarding claim 2, **Halperin** further teach a method comprising:

A) inhibiting a write or append operation associated with program in response to flagging the program (Paragraph 108).



The examiner notes that **Halperin** teaches **"inhibiting a write or append operation associated with program in response to flagging the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 5, **Halperin** further teaches a method comprising:

A) sending an alert in response to flagging the program (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"sending an alert in response to flagging the program"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 7, **Halperin** further teaches a method comprising:

A) sending an alert to a network monitoring system in response to flagging the program (Paragraph 111).

The examiner notes that **Halperin** teaches **"sending an alert to a network monitoring system in response to flagging the program"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 8, **Halperin** further teaches a method comprising:

A) logging any file system operations including recording a filename and a location where the local or shared file is written (Paragraph 108).

Art Unit: 2168

The examiner notes that **Halperin** teaches **“logging any file system operations including recording a filename and a location where the local or shared file is written”** as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be “quarantined” at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages” (Paragraph 108).

Regarding claim 9, **Halperin** teaches a method comprising:

- A) allowing a security level to be set (Paragraphs 43-44, 108, and 111);
- B) monitoring predetermined file system operations associated with a program (Abstract, Paragraphs 73-77, and 88-108); and
- C) logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written in response to the file being written (Paragraphs 108).

The examiner notes that **Halperin** teaches **“allowing a security level to be set”** as “In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan” (Paragraphs 43-44), “The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages” (Paragraph 108), and “Alternatively, different systems may have greater or lesser sensitivity levels,

Art Unit: 2168

or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that Halperin teaches **"monitoring predetermined file system operations associated with a program"** "Reference is now made to FIG. 6, which is a simplified flowchart illustration of an exemplary method of operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include...Attempting to contact previously unused or unknown IP addresses or IP Sockets" (Paragraphs 88-96), and "Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as "polymorphic viruses" may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that have the same or similar data, whether or not they have the same name" (Paragraph 97-106). The examiner further notes that Halperin teaches **"logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written in response to the file being written"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).



Art Unit: 2168

Regarding claim 12, **Halperin** further teaches a method comprising:

A) receiving a notification that the program intends to perform one of the predetermined file system operations (Paragraph 108).

The examiner notes that **Halperin** teaches **“receiving a notification that the program intends to perform one of the predetermined file system operations”** as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be “quarantined” at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages” (Paragraph 108).

Regarding claim 13, **Halperin** further teaches a method comprising:

A) following a predefined procedure in response to the level of security set (Paragraphs 43-44, 108, and 111).

The examiner notes that **Halperin** teaches **“following a predefined procedure in response to the level of security set”** as “In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan” (Paragraphs 43-44), “The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages” (Paragraph 108), and “Alternatively,



Art Unit: 2168

different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 14, **Halperin** further teaches a method comprising:

A) flagging the program in response to the program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"flagging the program in response to the program attempting to perform one of the predetermined file system operations"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 15, **Halperin** further teaches a method comprising:

A) flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

Art Unit: 2168

The examiner notes that Halperin teaches **“flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system”** as “A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network” (Abstract), “After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2” (Paragraph 97-107), and “server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected” (Paragraphs 73-77).

Regarding claim 16, Halperin further teach a method comprising:  
A) inhibiting any predetermined file system operations associated with program in response to the program being flagged (Paragraph 108).

The examiner notes that Halperin teaches **“inhibiting any predetermined file system operations associated with program in response to the program being flagged”** as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be “quarantined” at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period

Art Unit: 2168

may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 17, **Halperin** further teaches a method comprising:

A) sending an alert in response to the program attempting to perform any predetermined file system operations (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"sending an alert in response to the program attempting to perform any predetermined file system operations"** as "server 108 may initiate one or more virus containment actions such as, but not limited to: ...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 18, **Halperin** further teaches a method comprising:

A) sending the alert to a network monitoring system (Paragraph 111).

The examiner notes that **Halperin** teaches **"sending the alert to a network monitoring system"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 19, **Halperin** further teaches a method comprising:

A) presenting an alert to a user for approval before the predetermined file system operation is performed by the program (Paragraph 108).

The examiner notes that **Halperin** teaches **"presenting an alert to a user for approval before the predetermined file system operation is performed by the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

Regarding claim 21, **Halperin** teaches a system comprising:



Art Unit: 2168

- A) a file system protection program operable on a computer including: means to monitor predetermined file system operations associated with another program (Abstract, Paragraphs 73-77, and 88-108);
- B) a plurality of settable levels of security (Paragraphs 43-44, 108, and 111);
- C) a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security (Paragraphs 43-44, 108, and 111); and
- D) means to log any predetermined file system operations associated with the other program including recording a filename and location where a file is written after the file is written (Paragraph 108).

The examiner notes that Halperin teaches “**a file system protection program operable on a computer including: means to monitor predetermined file system operations associated with another program**” “Reference is now made to FIG. 6, which is a simplified flowchart illustration of an exemplary method of operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include...Attempting to contact previously unused or unknown IP addresses or IP Sockets” (Paragraphs 88-96), and “Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as “polymorphic viruses” may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that have the same or similar data, whether or not they have the same name” (Paragraph 97-106). The examiner further notes that Halperin teaches “**a plurality of settable levels of security**” as “In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan” (Paragraphs 43-44), “The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company



Art Unit: 2168

or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that Halperin teaches **"a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that Halperin teaches **"means to log any predetermined file system operations associated with the other program including recording a filename and location where a file is written after the file is written"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be

Art Unit: 2168

"quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 23, **Halperin** further teaches a system comprising:

A) a log to record any predetermined file system operations (Paragraphs 108 and 131).

The examiner notes that **Halperin** teaches "**a log to record any predetermined file system operations**" as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108) and "The present invention may be used to identify suspicious activity as it begins to spread within a first group and then receive a report of similar suspicious activity in a second group that is not a neighbor of the first group. In this case, the present invention may be used to analyze recent log files of communications between computing devices in the first and second groups. Since the groups are not neighbors, such communications are not likely to be found under normal circumstances. If a recent communication is identified between the two groups, this may be treated as a suspicious event. The communication may then be forwarded to a human operator for analysis to identify malicious software. In addition, this process may be used to identify

Art Unit: 2168

the specific communication message that is carrying the virus, which may lead to containment actions being taken" (Paragraph 131).

Regarding claim 24, **Halperin** further teaches a system comprising:

A) means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system; the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the other program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system; the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the other program attempting to write or append a remote file to the local file system"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 25, **Halperin** further teaches a system comprising:



Art Unit: 2168

A) means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **“means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations”** as “A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network” (Abstract), “After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2” (Paragraph 97-107), and “server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected” (Paragraphs 73-77).

Regarding claim 26, **Halperin** further teaches a system comprising:

A) means to send an alert in response to flagging the other program (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **“means to send an alert in response to flagging the other program”** as “server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected” (Paragraphs 73-77).

Regarding claim 27, **Halperin** further teaches a system comprising:

A) a network monitoring system (Paragraph 111); and

B) means to send an alert to the network monitoring system in response to flagging the other program (Paragraph 111)

The examiner notes that **Halperin** teaches **“a network monitoring system”** as “It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification” (Paragraph 111). The examiner further notes



Art Unit: 2168

that **Halperin** teaches **“means to send an alert to the network monitoring system in response to flagging the other program”** as “It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification” (Paragraph 111).

Regarding claim 28, **Halperin** further teach a system comprising:

A) means to inhibit predetermined file system operations associated with the other program in response to the other program being flagged (Paragraph 108).

The examiner notes that **Halperin** teaches **“means to inhibit predetermined file system operations associated with the other program in response to the other program being flagged”** as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be “quarantined” at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages” (Paragraph 108).

Regarding claim 29, **Halperin** further teaches a system comprising:

A) means to present an alert to a user (Paragraphs 73-77); and

B) means for the user to approve one of the predetermined file system operations before being performed by the other program (Paragraph 108).

The examiner notes that **Halperin** teaches **“means to send an alert in response to flagging the other program”** as “server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected” (Paragraphs 73-77). The examiner further notes that **Halperin** teaches **“means for the user to approve one of the predetermined file system operations before being performed by the other program”** as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses

Art Unit: 2168

before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

Regarding claim 30, **Halperin** teaches a method comprising:

- A) providing means to monitor predetermined file system operations associated with another program (Abstract, Paragraphs 73-77, and 88-108);
- B) defining a plurality of settable levels of security (Paragraphs 43-44, 108, and 111);
- C) providing a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security (Paragraphs 43-44, 108, and 111); and
- D) providing means to log any predetermined file system operations associated with the other program including recording a filename and location where a file is written in response to the file being written (Paragraph 108).

The examiner notes that **Halperin** teaches "**providing means to monitor predetermined file system operations associated with another program**"

"Reference is now made to FIG. 6, which is a simplified flowchart illustration of an exemplary method of operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include...Attempting to contact previously unused or unknown IP addresses or IP Sockets" (Paragraphs 88-96), and "Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as "polymorphic viruses" may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that have the same or similar data, whether or not they have the same name" (Paragraph 97-106). The examiner further notes that **Halperin** teaches "**defining a plurality of settable levels of security**" as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present

Art Unit: 2168

invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that Halperin teaches **"providing a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify



Art Unit: 2168

other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that Halperin teaches **"providing means to log any predetermined file system operations associated with the other program including recording a filename and location where a file is written in response to the file being written"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 32, Halperin further teaches a method comprising:

A) forming a log to record any predetermined file system operations (Paragraphs 108 and 131).

The examiner notes that Halperin teaches **"forming a log to record any predetermined file system operations"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other



Art Unit: 2168

organization versus internal messages" (Paragraph 108) and "The present invention may be used to identify suspicious activity as it begins to spread within a first group and then receive a report of similar suspicious activity in a second group that is not a neighbor of the first group. In this case, the present invention may be used to analyze recent log files of communications between computing devices in the first and second groups. Since the groups are not neighbors, such communications are not likely to be found under normal circumstances. If a recent communication is identified between the two groups, this may be treated as a suspicious event. The communication may then be forwarded to a human operator for analysis to identify malicious software. In addition, this process may be used to identify the specific communication message that is carrying the virus, which may lead to containment actions being taken" (Paragraph 131).

Regarding claim 33, **Halperin** further teaches a method comprising:

A) providing means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system; the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the other program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"providing means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system; the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the other program attempting to write or append a remote file to the local file system"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same

Art Unit: 2168

time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 34, **Halperin** further teaches a method comprising:

A) means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 35, **Halperin** further teaches a method comprising:

A) providing means to send an alert in response to flagging the other program (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"providing means to send an alert in response to flagging the other program"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 36, **Halperin** further teaches a method comprising:

A) providing a network monitoring system (Paragraph 111); and

Art Unit: 2168

B) providing means to send an alert to the network monitoring system in response to flagging the other program (Paragraph 111)

The examiner notes that **Halperin** teaches “**providing a network monitoring system**” as “It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification” (Paragraph 111). The examiner further notes that **Halperin** teaches “**providing means to send an alert to the network monitoring system in response to flagging the other program**” as “It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification” (Paragraph 111).

Regarding claim 37, **Halperin** further teaches a method comprising:

- A) providing means to present an alert to a user (Paragraphs 73-77); and
- B) providing means for the user to approve one of the predetermined file system operations before being performed by the other program (Paragraph 108).

The examiner notes that **Halperin** teaches “**providing means to send an alert in response to flagging the other program**” as “server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected” (Paragraphs 73-77). The examiner further notes that **Halperin** teaches “**providing means for the user to approve one of the predetermined file system operations before being performed by the other program**” as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be “quarantined” at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected” (Paragraph 108).

Regarding claim 38, **Halperin** teaches a computer-readable medium comprising:

- A) allowing a security level to be set on the computer (Paragraphs 43-44, 108, and 111);
- B) monitoring predetermined file system operations associated with a program (Abstract, Paragraphs 73-77, and 88-108); and



Art Unit: 2168

C) logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written in response to the file being written (Paragraphs 108).

The examiner notes that **Halperin** teaches **“allowing a security level to be set on the computer”** as “In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan” (Paragraphs 43-44), “The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages” (Paragraph 108), and “Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification” (Paragraph 111). The examiner further notes that **Halperin** teaches **“monitoring predetermined file system operations associated with a program”** “Reference is now made to FIG. 6, which is a simplified flowchart illustration of an exemplary method of operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include...Attempting to contact previously unused or unknown IP addresses or IP Sockets” (Paragraphs 88-96), and “Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as “polymorphic viruses” may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that



Art Unit: 2168

have the same or similar data, whether or not they have the same name" (Paragraph 97-106). The examiner further notes that **Halperin** teaches **"logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written in response to the file being written"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 40, **Halperin** further teaches a computer-readable medium comprising:

A) following a predefined procedure in response to the level of security set (Paragraphs 43-44, 108, and 111).

The examiner notes that **Halperin** teaches **"following a predefined procedure in response to the level of security set"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different

Art Unit: 2168

sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 41, **Halperin** further teaches a computer-readable medium comprising:

A) flagging the program in response to the program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"flagging the program in response to the program attempting to perform one of the predetermined file system operations"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 42, **Halperin** further teaches a computer-readable medium comprising:

A) flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the

Art Unit: 2168

local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that Halperin teaches **“flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system”** as “A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network” (Abstract), “After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2” (Paragraph 97-107), and “server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected” (Paragraphs 73-77).

Regarding claim 43, Halperin further teach a computer-readable medium comprising:

A) inhibiting any predetermined file system operations associated with program in response to the program being flagged (Paragraph 108).

The examiner notes that Halperin teaches **“inhibiting any predetermined file system operations associated with program in response to the program being flagged”** as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be “quarantined” at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a



Art Unit: 2168

computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 44, **Halperin** further teaches a computer-readable medium comprising:

A) sending an alert in response to the program attempting to perform any predetermined file system operations (Paragraphs 73-77).

The examiner notes that **Halperin** teaches "**sending an alert in response to the program attempting to perform any predetermined file system operations**" as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 3-4, 10-11, 20, 22, 31, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Halperin et al.** (U.S. PG PUB 2002/0194490) as applied to claims 1-2, 5, 7-9, 12-19, 21-30, 32-38, and 40-44, in view of **Satterlee et al.** (U.S. PG PUB 2004/0025015).

10. Regarding claim 3, **Halperin** does not explicitly teach a method comprising:  
A) monitoring all file operations associated with the program in response to the program not being in a safe list.

**Satterlee**, however, teaches "**monitoring all file operations associated with the program in response to the program not being in a safe list**" as "the present

Art Unit: 2168

invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 4, **Halperin** does not explicitly teach a method comprising:  
A) permitting selected read and write operations in response to a predefined rules table.

**Satterlee**, however, teaches "**permitting selected read and write operations in response to a predefined rules table**" as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 10, **Halperin** does not explicitly teach a method comprising:  
A) selecting a program for monitoring in response to the program not being on a safe list.

**Satterlee**, however, teaches "**selecting a program for monitoring in response to the program not being on a safe list**" as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an

Art Unit: 2168

harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 11, **Halperin** further teaches a method comprising:

A) logging any file system operations (Paragraph 108).

The examiner further notes that **Halperin** teaches “**logging any file system operations**” as “In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be “quarantined” at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages” (Paragraph 108).

**Halperin** does not explicitly teach:

A) associated with any programs on the safe list.

**Satterlee**, however, teaches “**associated with any programs on the safe list**” as “the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities” (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee’s** would have allowed **Halperin’s** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 20, **Halperin** further teaches a method comprising:

A) requiring approval before performing any predetermined file system operations associated with the program (Paragraph 108).

The examiner notes that **Halperin** teaches “**requiring approval before performing any predetermined file system operations associated with the program**” as “In this way, should a computer virus send one or more infected



Art Unit: 2168

messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

**Halperin** does not explicitly teach:

A) in response to the program not being on a safe list.

**Satterlee**, however, teaches "**in response to the program not being on a safe list**" as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 22, **Halperin** does not explicitly teach a system comprising:

A) a safe list; and

B) wherein the file system program is adapted to monitor the other program in response to the other program not being on the safe list.

**Satterlee**, however, teaches "**a safe list**" as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13), and "**wherein the file system program is adapted to monitor the other program in response to the other program not being on the safe list**" as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an

Art Unit: 2168

harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 31, **Halperin** does not explicitly teach a method comprising:

- A) providing a safe list; and
- B) adapting the file system protection program to monitor the other program in response to the other program not being on the safe list.

**Satterlee**, however, teaches “**providing a safe list**” as “the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities” (Paragraph 13), and “**adapting the file system protection program to monitor the other program in response to the other program not being on the safe list**” as “the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities” (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee’s** would have allowed **Halperin’s** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 39, **Halperin** does not explicitly teach a method comprising:

- A) selecting the program for monitoring in response to the program not being on a safe list.

**Satterlee**, however, teaches “**selecting the program for monitoring in response to the program not being on a safe list**” as “the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities” (Paragraph 13) and “predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat” (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee’s** would have allowed **Halperin’s** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

### ***Response to Arguments***

Art Unit: 2168

11. Applicant's arguments filed 09/04/2007 have been fully considered but they are not persuasive.

Applicant argues on page 13 that **"Halperin does not teach or suggest flagging a program on a computer as being suspect for possible containing a virus"**. However, the examiner wishes to refer to paragraphs 73-77 of **Halperin** which state "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77). The examiner further wishes to state that notifying a user at a specific computer 100 that there is a possible virus on that specific computer (see "Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected") teaches flagging a suspected malicious program on a specific computer.

Applicant argues on pages 13 and 15 that **"nor does Halperin teach or suggest the specific conditions associated with the computer for flagging the program on the computer as provided by the embodiment of the present invention as recited in claim 1"** and **"Halperin does not teach or suggest the specific conditions or file system operations...as recited in claim 1"**. However, the examiner wishes to state that only one of the four operations is required to be taught by **Halperin** due to the "at least one of" language of the independent claims. Moreover, the examiner wishes to refer to paragraph 73 of **Halperin** which states that "As the virus attempts to propagate it selects one or more valid and decoy addresses from address book 102 and folders 104, automatically generates messages that incorporate the virus, typically as an attachment, and forwards the messages to server 108" (Paragraph 73). The examiner further wishes to state that the limitation "the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system" is taught by the aforementioned citation of **Halperin**. Specifically, the virus of **Halperin** reads or opens itself up by being functionally active in performing malicious activity. Moreover, by attaching a copy of itself in a e-mail message, the virus teaches writing or appending any content to the local file on the local file system.

Applicants argue on page 14 that **"Halperin teaches suspending message being sent by an infected computer but Halperin does not teach or suggest flagging a program on the computer based on specific local file system operations as provided by the embodiment of the present invention"**. However, the examiner wishes to state that only one of the four operations is required to be taught by **Halperin** due to the "at least one of" language of the independent claims. Moreover, the examiner wishes to refer to paragraph 73 of **Halperin** which states that "As the virus attempts to propagate it selects one or more valid and decoy addresses from address book 102 and folders 104, automatically generates messages that incorporate the virus, typically as an attachment, and forwards the messages to server 108" (Paragraph 73). The examiner further wishes to state that the limitation "the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on



Art Unit: 2168

the local file system" is taught by the aforementioned citation of **Halperin**. Specifically, the virus of **Halperin** reads or opens itself up by being functionally active in performing malicious activity. Moreover, by attaching a copy of itself in a e-mail message, the virus teaches writing or appending any content to the local file on the local file system. Furthermore, by sending the e-mail message to a decoy address (the act of sending something is a local operation) the resultant suspicion and flagging through notification occurs.

Applicant argues on page 15 that **"Applicant respectfully submits that there is no teaching or suggestion in Halperin of flagging a program on an individual computer as being suspect for possibly containing a virus"**. However, the examiner wishes to refer to paragraphs 73-77 of **Halperin** which state "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77). The examiner further wishes to state that notifying a user at a specific computer 100 that there is a possible virus on that specific computer (see "Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator of a specific computer that a virus may have been detected") teaches flagging a suspected malicious program on a specific computer.

Applicant argues on page 16 that **"Applicant respectfully submits that Halperin teaches away from the present invention in that Halperin quarantines the messages and does not allow them to reach their intended destinations. In contrast, the present invention, as recited in the embodiment of claim 1, permits the file to be copied or written by the program at its intended location and then stores the file name and location where the local or shared file is copied or written"**. However, the Applicants are also reminded that in order to disqualify a reference based on a "teach away" reasoning, the reference has to explicitly suggest or disclose the so-called teach away steps - Applicants assertion can not be accepted if it is unsupported by a valid evidence. In this case, **Halperin** does teach the writing of the e-mail message by the virus that, as a result, teaches the operations recited in the independent claims. Moreover, because **Halperin** teaches the recognition of the decoy address and the notification of the user of the specific computer of a potential virus, he teaches the location of where the e-mail was written and where it was intended to be sent. Furthermore, by quarantining the entire e-mail message (including its filename), **Halperin** teaches storing the filename of the message.

Applicant argues on page 19 that **"Applicant respectfully submits that there is no teach or suggesting in Halperin and Satterlee that their teachings may be combined so as to provide the present invention as recited in the claims"**. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958

Art Unit: 2168

F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both **Satterlee** and **Halperin** deal with virus protection, and as a result, can be combined.

### **Conclusion**

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 6,886,099 issued to **Smithson et al.** on 26 April 2005. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,735,700 issued to **Flint et al.** on 11 May 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2002/0116639 issued to **Chefalas et al.** on 22 August 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,973,578 issued to **McIchione** on 06 December 2005. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,357,008 issued to **Nachenberg** on 12 March 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2002/0174358 issued to **Wolff et al.** on 21 November 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2004/0015712 issued to **Szor** on 22 January 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2002/0178375 issued to **Whittaker et al.** on 28 November 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2003/0204569 issued to **Andrews** on 30 October 2003. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2005/0268112 issued to **Wang et al.** on 01 December 2005. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2004/0030913 issued to **Liang et al.** on 12 February 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2004/0098607 issued to **Alagna et al.** on 20 May 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 20020194489 issued to **Almogly et al.** on 19 December 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

Art Unit: 2168

U.S. PGPUB 2002/0188649 issued to **Karim** on 12 December 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,901,519 issued to **Stewart et al.** on 31 May 2005. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 7,093,239 issued to **van der Made** on 15 August 2006. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 5,623,600 issued to **Ji** on 22 April 1997. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,763,462 issued to **Marsh** on 13 July 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 5,257,381 issued to **Cook** on 26 October 1993. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

#### **Contact Information**

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mahesh Dwivedi whose telephone number is (571) 272-2731. The examiner can normally be reached on Monday to Friday 8:20 am – 4:40 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim Vo can be reached (571) 272-3642. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

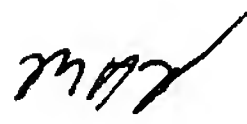
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Application/Control Number: 10/710,477  
Art Unit: 2168

Page 36

Mahesh Dwivedi  
Patent Examiner  
Art Unit 2168

  
November 08, 2007



TIM VO  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100